Iran's Emergence as a Cyber Power

August 20, 2014 | LTC Eric K. Shafa

> Iran is a country of 80 million people, educated and dynamic. It sits astride a crucial part of the world. It cannot be sanctioned and pressed down forever. It is the last great civilization to sit outside the global order.
>
> Fareed Zakariaa[1]

As international scrutiny remains focused on the Islamic Republic of Iran's nuclear program, a capability is developing in the shadows inside Iran that could pose an even greater threat to the United States. The *2010 National Security Strategy* discusses Iran in the context of its nuclear program, support of terrorism, its influence in regional activities, and its internal problems. There was no mention of Iran's cyber capability or of that ability to pose a threat to U.S. interests. This is understandable, considering Iran has not been a major concern in the cyber realm. Furthermore, Russia and China's cyber activities have justifiably garnered a majority of attention and been widely reported in the media over the past decade. Iran's cyber capabilities have been considered third-tier at best. That is rapidly changing. This report discusses the growing cyber capability of Iran and why it poses a new threat to U.S. national interests.

Iran in a Cyber Context.

Just as computing power grows exponentially each year, so can an adversary's cyber capabilities. When one considers the origins of world-class cyber threats to the United States, two countries immediately come to mind—Russia and China. Yet with its growing cyber capabilities and intent to use them, Iran is rapidly striving to earn a position among the ranks of this

nefariously elite group. For decades, the U.S. Government has publicly acknowledged concern over Iran's efforts to develop a nuclear program to counter U.S. military capabilities. Recently, the 2014 *Quadrennial Defense Review* stated that, "Over the past 5 years, a top Administration priority in the Middle East has been preventing Iran from acquiring a nuclear weapon."[2] This focus on Iran's nuclear ambitions has distracted many from Iran's other developing capability. In the last few years, Iran's cyber proficiency has garnered the attention of a select few government officials and private industry leaders. In late-2011, the executive chairman of Google stated, "The Iranians are unusually talented in cyber war for some reason we don't fully understand."[3] Stopping a cyber adversary from disrupting activity or stealing intellectual property has been the primary concern of government and private sector organizations, but in the military and intelligence communities, there are other concerns about Iran.

Few countries (or nonstate actors) can come close to matching or opposing U.S. military capabilities without taking an asymmetric warfare approach. As U.S.-led sanctions and international isolation impact Iran, the regime continues to seek ways to counter this threat and send a message. "The past year [2012] has seen the Iranian regime evolve significantly in its exploitation of cyberspace as a tool of internal repression…Iran has also demonstrated a growing ability to hold Western targets at risk in cyberspace, amplifying a new dimension in asymmetric conflict."[4] In the global community, few countries are on par with the cyber capabilities of the United States, Russia, and China. The ability to attack another country or target an adversary's leaders, population, or infrastructure via the cyber domain, causing significant harm, disability, or damage to key facilities such as electric power grids or financial institutions has been the province of an elite group of countries. Iran, considered a third tier cyber power compared to the United States, is rapidly becoming a world-class cyber threat. During a recent subcommittee hearing, U.S. Representative Peter Hoekstra (R-Michigan) stated that, "Iran has boosted its cyber capabilities in a surprisingly short amount of time and possesses the ability to launch successful cyber attacks on American financial markets and its infrastructure."[5]

Iran's Cyber Evolution.

Any mention of the Islamic Republic of Iran immediately invokes thoughts of veiled nuclear programs and support for terrorism, as well as ways (primarily military) to counter these threats. However, understanding Iran's perspective is vital to knowing what is behind its cyber development. First and foremost in importance to the Islamic Republic is its regime survival, followed by its right to a nuclear program and other national interests. Prior to 2009, much of

Iran's cyber efforts were focused internally on countering government dissidence. The influential Iranian Revolutionary Guard Corp (IRGC) proposed the development of an Iranian Cyber Army in 2005 to combat internal threats. It sought out professional hackers through voluntary means or by using blackmail and threats to boost its ranks.

Although the 2007 Russian cyber attacks against the government websites of Estonia and Georgia may have been the first such shots in cyberspace, the Stuxnet attack that targeted Iran's nuclear infrastructure was the catalyst that changed the entire dynamic of Iranian cyber development. Publicly revealed in July 2010, it is considered the most advanced cyber weapon of its kind to date. Stuxnet insidiously compromised centrifuge operations at the Natanz nuclear power plant critical to Iran's uranium enrichment efforts, causing delays to Iran's nuclear program. Ironically, Stuxnet also served as the watershed event that spurred the Islamic Republic to make Iran's cyber capability a priority. From an Iranian perspective, Stuxnet was like the famous bifurcated sword called Dhu al-Fiqar or Zolfaqar in Persian that, among Shia Muslims, is believed to have been given by the Islamic prophet Muhammad on his death bed to his son-in-law Ali as his successor. Stuxnet confirmed that the Islamic Republic's interests were under attack, but it also served as the forcing function needed to formalize and expand its cyber capability.[6]

In early March 2012, Supreme Leader of Iran Ayatollah Ali Khameni publicly announced to state media the creation by decree of a new Supreme Council of Cyberspace charged "to oversee the defense of the Islamic Republic's computer networks and develop new ways of infiltrating or attacking the computer networks of its enemies."[7] It included heads of intelligence, militia, security, media chiefs, and the IRGC. It has its own budget and offices along with the power to enact laws. Additionally, the IRGC stated that a secure internal network for high-level command and control called "Basir" (Persian for perceptive) was created to counter outside threats to online activities.[8] However, it is clear from its actions against opposition influences and dissident groups that the regime continues internal censorship and monitoring as well. Furthermore, Reporters Without Borders, in its 2012 annual report of countries that restrict internet access, filter content, and imprison bloggers, "ranked Iran the number one enemy of the Internet…ahead of 11 other countries—including Saudi Arabia, Bahrain, Syria, China, and Belarus."[9]

Today, Iran as a cyber power is the elephant in the room that everyone is finally beginning to notice. The Iranian government was originally believed to have budgeted approximately $76 million annually to its fledgling cyber force. However, in late-2011, Iran invested at least $1 billion dollars in cyber technology, infrastructure, and expertise.[10] In March 2012, the IRGC claimed it

had recruited around 120,000 personnel over the past 3 years to combat "a soft cyber war against Iran."[11] In early-2013, an IRGC general publically claimed Iran had the "fourth biggest cyber power among the world's cyber armies."[12] Regardless of the numbers, the fact is that Iran's cyber capability continues to mature. The IRGC has its own Cyber Defense Command which recruits and trains cyber warriors to spy on dissidents on the internet and spread Iranian government propaganda.[13] The IRGC also now owns and controls Iran's largest communication company and manages the skilled cyber technicians and specialists of Iran's Cyber Army trained to hack into opposition websites and conduct other types of offensive cyber operations. On the law enforcement side, the FETA police (in Persian it literally means Police of the Space of Creating and Exchanging Information) handle typical internet crimes as well as more opaque enforcement activities such as political and security crimes. There are other Iranian organizations and companies recruited and/or affiliated with Iran's cyber capabilities, either knowingly or by loose association.

On February 12, 2013, during a discussion about Iran's cyber development at the Center for National Security at Fordham Law, former Iranian Ambassador and visiting current research scholar at Princeton University Seyed Hossein Mousavian stated, "The U.S., or Israel, or the Europeans, or all of them together, started war…Iran decided to establish a cyber army, and today, after 4 or 5 years, Iran has one of the most powerful cyber armies in the world…it's exaggerating the present capabilities but it's working toward the future."[14] While Iran's overall cyber capabilities may be inflated there is little doubt it is serious about becoming a dominant future cyber power. That future may be closer than initially anticipated. General William Shelton, head of the U.S. Air Force Space Command, said "Iran's developing ability to launch cyber attacks will make it a force to be reckoned with. Iran poses a risk because of the potential capabilities that they will develop over the years and the potential threat that will represent to the U.S."[15]

Iran's Cyber Capability as a Threat.

While Iran has not yet graduated to full membership as a world-class cyber power on par with the United States, China, and Russia, "it is the intensity, variety, and destructiveness of Iran-linked cyber intrusions over the past 5 years" that has accelerated its ranking as a cyber threat.[16] The evolution of Iranian cyber capability did not just occur overnight or in a vacuum. It was cultivated over the years in a crucible of real-world activity and consolidated in lessons learned from dealing with internal attacks against the government by dissidents, external attacks against its nuclear infrastructure, and through efforts to create and educate its own technical force. What Iran currently lacks in technological know-how, it more than makes up for in ambition. To reinforce

this point and show Iran's intent, the commander of Iran's information technology and communication department of the General Staff of the Iranian Armed Forces stated that "one of the options on the table of the U.S. and its allies is a cyber war against Iran…but we are fully prepared to fight cyber warfare."[17]

The sophistication of attacks like Stuxnet proved successful in delaying Iran's nuclear program development, but it also served as an opening salvo in the escalation of cyber warfare. "Iran represents a qualitatively different cyber actor…[t]hey're not stealing our intellectual property en masse like China, or using cyberspace as a black market like the Russians do…what Iran does use cyber for, including elevating its retaliatory capabilities abroad, makes it a serious threat."[18] Iran understands it cannot match the United States and its allies directly and therefore must strengthen its asymmetric toolset to counterbalance this gap. So as not to rely exclusively on foreign technology, in late December 2013, the IRGC publically revealed indigenously developed cyber defense products including secure: cell phones; operating system; navigation system; telecommunications optical transmission system; anti-malware; cyber threats recognition and identification system; security operations center; a high-speed and high-capacity firewall and a software firewall. Although the technology is likely not as advanced as U.S. equipment, this proves that the Islamic Republic is tenaciously working to address its concerns and close the gap.

Iran is actively seeking increased offensive cyber capabilities that could also increase its asymmetric position. It has shown its ability to use cyber attacks to infiltrate and take down targets. In 2011, it infiltrated a Dutch company and stole digital certificates for secure communications that it later used internally to hack Iranian citizens' communications and email. In 2012, Iran was suspected of launching malware that wreaked havoc on 30,000 computers at the Saudi oil company Aramco. This attack was followed later in the year by another against Qatari energy company, RasGas. In late-2012, a significant Distributed Denial of Service (DDOS) attack was executed against websites of major U.S. banks. Iran was suspected, but what was even more disconcerting to the United States, was the magnitude of traffic flow which was greater than anything previously seen from a DDOS attack up to that point. This indicated a remarkable degree of sophistication.[19] In late-2013, Iran's infiltration of the U.S. Navy's internet network garnered much attention because it indicated Iran's capability had advanced. It not only showed Iran could get into a U.S. Department of Defense system, but it highlighted the ability to stay in it for several months. An example of this improved knowledge was initially suggested back in May 2012 when Morteza Rezaei, an Iranian cyber engineer with NEDA Industrial Group in Tehran, published his analysis of how to defend against Stuxnet.[20] What was more disturbing was he wrote it in *Control*

Global, a U.S. publication, to show just how far Iran's cyber knowledge had come.

Iran is no doubt working hard to elevate its standing as a world-class cyber power. It is taking full advantage of U.S. foreign policy issues to foster relationships with U.S. adversaries such as China and Russia that will help advance Iran's cyber capabilities. General Martin Dempsey, Chairman of the Joint Chiefs of Staff, stated in an interview in January 2013 that, "there are reports that destructive cyber tools have been used against Iran…whoever's using those can't assume that they're the only smart people in the world."[21] Maybe a more imminent U.S. concern regarding Iran should be the danger the Islamic Republic poses if it becomes a world-class cyber power. All indications show this is likely to happen sooner than later.

ENDNOTES

1. Fareed Zakaria, "To Deal with Iran's Nuclear Future, Go Back to 2008," *The Washington Post*, October 26, 2011.

2. *2014 Quadrennial Defense Review*, Washington, DC: Department of Defense, 2014, p 21.

3. Eric Schmidt, during CNN interview with Erin Burnett that aired on December 15, 2011.

4. Iian Berman, "The Iranian Cyber Threat, Revisited," Statement before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Washington, DC, March 20, 2013.

5. Peter Hoekstra, House Committee on Foreign Affairs, Joint Subcommittee Hearing: Iran's Support for Terrorism Worldwide, Washington, DC: March 4, 2014.

6. Tony Capaccio, "Iran's Cyber Threat Potential Great, U.S. General Says," Bloomberg, January 17, 2013.

7. Shane Harris, "Forget China: Iran's Hackers Are America's Newest Cyber Threat," *Foreign Policy*, February 18, 2014.

8. Farnaz Fassihi, "Iran's Censors Tighten Grip," *The Wall Street Journal*, March 16, 2012.

9. *Ibid*.

10. Ashley Wheeler, "Iranian Cyber Army, The Offensive Arm of Iran's Cyber Force," September 2013, available from *www.phoenixts.com/blog/iranian-cyber-army*.

11. Fassihi, p. 2.

12. "Iran Enjoys 4th Biggest Cyber Army in the World," FARS (Tehran), February 2, 2013.

13. "After the Green Movement: Internet Controls in Iran 2009-2012," Open Net Initiative, February 2013, available from *https://opennet/sites/opennet.net/files/iranreport.pdf*.

14. Center on National Security at Fordham Law, discussion with Seyed Hossein Mousavian and Robert Windrem, February 12, 2013, available from *www.centeronnationalsecurity.org*.

15. Capaccio, p.1.

16. Mark Clayton, "Cyber-war: In Deed and Desire, Iran Emerging as a Major Power," *The Christian Science Monitor*, March 16, 2014.

17. "Commander Reiterates Iran's Preparedness to Confront Enemies in Cyber Warfare," Tasnim News Agency (Tehran), February 18, 2014.

18. Clayton, p. 3.

19. Harris, p. 1.

20. Clayton, p. 4.

21. Harris, p. 2.

*****

*****